早稲田大学大学院 理工学研究科

博 士 論 文 概 要

論 文 題 目

Provably Secure Digital Signatures with Additional Property

証明可能安全な機能付きディジタル署名方式

申 請 者

駒野	雄一
Yuichi	Komano

２００７年 ５月

本論文では、情報セキュリティ分野における付加機能を有するディジタル署名方式とその安全性をモデル化し、証明可能安全な方式の提案を行う。

公開鍵暗号やディジタル署名の安全性は、多項式時間 Turing 機械である攻撃者をブラックボックスとみなし、攻撃者の動作環境（攻撃シナリオ）と目的（被害の大きさ）により定式化される。

近年、安全かつ効率的な公開鍵暗号方式やディジタル署名方式に加え、応用に即した付加機能を有する公開鍵暗号やディジタル署名が多数提案されている。付加機能を有する方式は、各々について適切に安全性を定式化する必要がある。本論文では、以下の４種類の機能付き署名方式について安全性をモデル化し、証明可能安全な方式の構成を論ずる。本論文で構成される方式により、インターネット上でのアプリケーション等を安全かつ効率的に実現できるようになるほか、新たな付加機能を有する方式の開発における安全性の定式化の礎となることが期待される。

1. 複数の署名者間での公平な署名交換を実現する方式
2. 複数の署名者が稟議形式で署名を生成して署名長を削減する方式
3. 肯定／否認付加機能をもつ匿名署名方式
4. 公開鍵暗号とディジタル署名を同一のフレームワークで実現する方式

以下に各項の詳細をまとめる。

1. 複数の署名者間での公平な署名交換を実現する方式

二者間で公平に署名を交換する方法として Chen らは Concurrent 署名とその安全性の概念をモデル化し、具体的な方式を提案した。樋渡らは、Concurrent 署名の概念を拡張して一対多で公平に署名を交換する概念とその安全性をモデル化して具体的な方式を提案したが、多の中に信頼できる署名者を仮定する必要があり、多対多では公平に署名を交換することはできなかった。

本論文では、多重署名方式の概念を利用することで、一対多および多対多で公平な署名を交換する方法とその安全性をモデル化し、ランダムオラクルモデルの下で離散対数問題の計算困難性を安全性の根拠として証明可能安全な方式を構成した。本方式は、同報通信路が必要となるものの、信頼できる署名者の仮定を排除することができる。さらに、樋渡らの方式よりも管理すべき情報が少なく、署名長を削減することができる。

2. 複数の署名者が稟議形式で署名を生成して署名長を削減する方式

板倉らは、個々の署名を連結したものよりも短い署名長で複数の署名者の承認を保証する方法として、複数の署名者が協力して一つの署名を生成する多重署名

方式の概念と具体的な方式を提案した。しかし、内部攻撃者に対する安全性など、安全性のモデルは経験的にのみ議論されてきた。

本論文では、グループ署名方式の安全性のモデルを参考にして多重署名方式の安全性のモデル化を再定義した。さらに、ランダムオラクルモデルの下で、落とし戸付き一方向性置換の一方向性を安全性の根拠とする二つの具体的な方式を提案した。そのうちの一つは、署名対象文書を多重署名の初期値に埋め込むことで、署名対象文書が一定サイズよりも大きいときに、同等の安全性を保証する公知技術の中で最も総通信量を小さくすることができる。また、メタ帰着の概念を利用して確率的な多重署名方式で用いる乱数成分の最適長を評価した。さらに、クローフリー置換対を用いる確定的な多重署名方式を提案し、ランダムオラクルモデルの下で安全性を証明している。クローフリー置換対を用いる多重署名方式は、安全性を保証するために落とし戸付き一方向性置換を利用する多重署名方式よりも制約された仮定を必要とするが、署名長を削減することが可能である。

3. 肯定／否認付加機能をもつ匿名署名方式

Rivestらは、署名者が他の複数のエンティティの公開鍵と自らの秘密鍵を利用することで、公開鍵に対応するエンティティあるいは秘密鍵をもつ署名者のうちの一人が承認した事実のみを保証することができるリング署名方式の概念と具体的な方式を提案した。しかし、リング署名方式は署名者の完全な匿名性を有するため、公開鍵に対応するエンティティに署名生成事実の責任を転嫁できるほか、署名者が後に権利主張する場合には署名生成時に利用した乱数成分を秘密裏に保持しておく必要があった。

本論文では、検証者と知識を証明する対話を行うことで、公開鍵が利用されたエンティティは署名生成事実を否認できるが肯定できず、署名者本人は署名生成事実を肯定できるが否認できない方法とその安全性をモデル化し、ランダムオラクルモデルの下で判定 Diffie-Hellman 問題が計算困難なときに証明可能安全な方式を構成した。本方式は、署名者本人がプライバシ情報の開示範囲や時期を制御することができる。

4. 公開鍵暗号とディジタル署名を同一のフレームワークで実現する方式

RSA 暗号や RSA 署名などの安全性を強化するために、暗号方式用のパディング手法である OAEP（Optimal Asymmetric Encryption Padding）や署名方式用のパディング手法である PSS（Probabilistic Signature Scheme）が提案されている。これらの前処理を用いた RSA-OAEP（OAEP のパディング処理結果に RSA 暗号を適用）や RSA-PSS（PSS のパディング処理結果に RSA 署名を適用）は、それぞれランダムオラクルモデルで RSA 問題の計算困難性を根拠として最強の安全性を証明できる。しかし、暗号方式と署名方式のそれぞれでパディング処理

が異なるため、両方式を実現するには二種類のパディング処理を実装しなければならないほか、安全性を保証するためには両方式で異なる鍵の組を準備する必要があった。Coron らは、暗号と署名で同一のパディング処理を利用する汎用的パディング（単一のパディング処理結果に RSA 暗号または RSA 署名などを適用）の概念をモデル化し、署名方式 PSS のパディング処理を利用して具体的な方法を提案したが、安全性証明における帰着効率が良い方法ではなかったため、安全性を保証するためには十分に長い鍵を用いる必要があった。

本論文では、暗号方式用のパディング手法である OAEP、OAEP++、REACT（Rapid Enhanced-security Asymmetric Cryptosystem Transform）を利用することで帰着効率の良い三種類の汎用パディング処理を構成する。特に、OAEP++、REACT を利用する二つの手法は、暗号方式・署名方式のいずれにおいても安全性証明における帰着効率が良いため、Coron らの手法よりも安全性を損なうことなく鍵サイズ（暗号文・署名サイズ）を抑えることができる。

研　究　業　績

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
1.論文○	Yuichi Komano, ``Fair Exchange of Signatures with Multiple Signers,'' IEICE Trans. on Fundamentals, Vol.E90-A No.5, 2007.5 (掲載予定)
2.論文○	Yuichi KOMANO, Kazuo OHTA, Atsushi SHIMBO, Shinichi KAWAMURA, ``Toward the Fair Anonymous Signatures: Deniable Ring Signatures, '' IEICE Trans. on Fundamentals, Vol.E90-A No.1, pp.54-64, 2007.1
3.論文○	Yuichi KOMANO, Kazuo OHTA, Atsushi SHIMBO, Shinichi KAWAMURA, ``Formal Security Model of Multisignatures,'' Information Security Conference 2006 (ISC'06), Samos-Greece, 2006.8
4.論文○	Yuichi KOMANO, Kazuo OHTA, ``Taxonomical Security Consideration of OAEP Variants, '' IEICE Trans. on Fundamentals, Vol.E89-A No.5, pp.1233-1245, 2006.5
5.論文○	Yuichi KOMANO, Kazuo OHTA, Atsushi SHIMBO, Shinichi KAWAMURA, ``Toward the Fair Anonymous Signatures: Deniable Ring Signatures,'' RSA Conference 2006, Cryptographers' Track (CT-RSA 2006), 2006.2
6.論文○	Yuichi KOMANO, Kazuo OHTA, Atsushi SHIMBO, Shinichi KAWAMURA, ``On the Security of Probabilistic Multisignature Schemes and their Optimality,'' International Conference on Cryptology in Malaysia (Mycrypt 2005), 2005.9
7.論文○	Yuichi KOMANO, Kazuo OHTA, ``Taxonomic Consideration to OAEP Variants and Their Security,'' Sixth International Conference on Information and Communications Security (ICICS'04), 2004.10
8.論文○	Yuichi KOMANO, Kazuo OHTA, ``OAEP-ES -- Methodology of Universal Padding Technique --,'' IEICE Trans. on Fundamentals, Vol.E87-A No.1, pp. 110-119, 2004.1
9.論文○	Yuichi KOMANO, Kazuo OHTA, ``Efficient Universal Padding Techniques for Multiplicative Trapdoor One-way Permutation,'' Advances in Cryptology CRYPTO 2003, 2003.8
10. 総説	駒野 雄一、``ディジタル署名の証明可能安全性と方式設計への帰還''、電子情報通信学会誌、2007 年 6 月 (掲載予定)
11. 講演	駒野 雄一、``ディジタル署名の証明可能安全性''、電子情報通信学会チュートリアル講演 (暗号技術の証明可能安全性)、2005 年 5 月

12. 講演	駒野 雄一、太田 和夫、新保 淳、川村 信一、``否認可能リング署名方式を用いた英国型匿名オークション方式''、2007 年暗号と情報セキュリティシンポジウム (SCIS 2007)、2007 年 1 月
13. 講演	駒野 雄一、``マルチパーティモデルでの公平な署名交換''、電子情報通信学会情報セキュリティ研究会 (ISEC)、2006 年 5 月
14. 講演	駒野 雄一、``プライバシ保護機能をもつ電子署名方式''、公開鍵暗号の安全な構成とその応用ワークショップ、東京大学生産技術研究所、2006 年 2 月
15. 講演	駒野 雄一、太田 和夫、新保 淳、川村 信一、``落し戸付き一方向性置換を利用する多重署名方式の最適性の再評価''、2006 年暗号と情報セキュリティシンポジウム (SCIS 2006)、 2006 年 1 月
16. 講演	駒野 雄一、太田 和夫、新保 淳、川村 信一、`` Claw-free 置換に基づく多重署名方式''、2005 年コンピュータセキュリティシンポジウム(CSS 2005)、2005 年 10 月
17. 講演	駒野 雄一、太田 和夫、新保 淳、川村 信一、``否認機能を持つリング署名方式の再考 (その 2)''、電子情報通信学会情報セキュリティ研究会 (ISEC)、2005 年 5 月
18. 講演	駒野 雄一、太田 和夫、新保 淳、川村 信一、``利用者のプライバシ保護を強化したブラインド署名方式''、電子情報通信学会 2005 年総合大会、2005 年 3 月
19. 講演	駒野 雄一、太田 和夫、新保 淳、川村 信一、``否認機能を持つリング署名方式の再考''、2005 年暗号と情報セキュリティシンポジウム (SCIS 2005)、2005 年 1 月
20. 講演	駒野 雄一、太田 和夫、新保 淳、川村 信一、``確率的多重署名方式に用いる乱数成分の最適長評価''、電子情報通信学会 2004 年ソサイエティ大会、2004 年 9 月
21. 講演	駒野 雄一、太田 和夫、`` ES 方式の通信効率に関する再考察''、電子情報通信学会 2004 年総合大会、2004 年 3 月
22. 講演	駒野 雄一、太田 和夫、川村 信一、新保 淳、``署名長増加を抑えた多重署名方式の構成'' 2004 年暗号と情報セキュリティシンポジウム (SCIS 2004)、2004 年 1 月
23. 講演	駒野 雄一、河内 恵、太田 和夫、多田 充、``落し戸付一方向性置換向けの署名順番可変な多重署名方式''、2004 年暗号と情報セキュリティシンポジウム (SCIS 2004)、2004 年 1 月
24. 講演	駒野 雄一、山崎 太郎、太田 和夫、`` XOAEPX-** -- OAEP の変形可能性につい

	て --'' 電子情報通信学会情報セキュリティ研究会（ISEC)、2003 年 3 月
25. 講演	駒野 雄一、太田 和夫、``REACT-ES & OAEP++-ES -- 更に有効な落し戸付き乗法的一方向性関数向け万能 Padding 方式 --'' 電子情報通信学会情報セキュリティ研究会（ISEC)、2003 年 3 月
26. 講演	駒野 雄一、山崎 太郎、太田 和夫、``OAEP-** --OAEP の変形可能性について（一方向性関数の場合）--'' 2003 年暗号と情報セキュリティシンポジウム（SCIS 2003、2003 年 1 月
27. 講演	駒野 雄一、太田 和夫、``OAEP-ES -- 落し戸付き乗法的一方向性関数に有効な効率的万能 Padding 方式--'' 2003 年暗号と情報セキュリティシンポジウム（SCIS 2003)、2003 年 1 月
28. 講演	駒野 雄一、太田 和夫、`` OAEP 暗号系の再評価+''、電子情報通信学会情報セキュリティ研究会（ISEC)、2002 年 11 月
29. 講演	駒野 雄一、太田 和夫、``署名の安全性証明技法の比較''、2002 年暗号と情報セキュリティシンポジウム（SCIS 2002)、2002 年 1 月